(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 102 00 681 A 1**

(51) Int. Cl.[7]:
G 06 F 12/14
G 05 B 19/042

(21) Aktenzeichen: 102 00 681.4
(22) Anmeldetag: 10. 1. 2002
(43) Offenlegungstag: 31. 7. 2003

DE 102 00 681 A 1

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Schlemper, Michael, 91056 Erlangen, DE;
Schlereth, Michael, 91452 Wilhermsdorf, DE

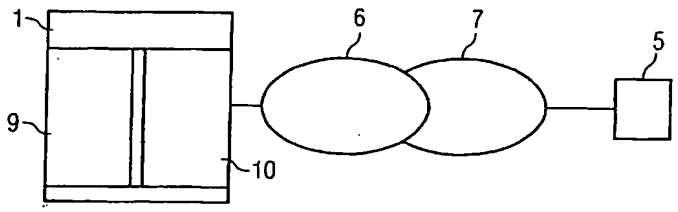
(56) Entgegenhaltungen:
WO 01 17 310 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Temporäre Zugansberechtigung zum Zugriff auf Automatisierungseinrichtungen

(57) Zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät auf eine Automatisierungseinrichtung, die über eine physikalische Netzwerkverbindung miteinander verbunden sind, verfügt die Automatisierungseinrichtung erfindungsgemäß über einen Zugriffsschutz, der in einem Grundzustand jeden Zugang über die Netzwerkverbindung abweist. Auf eine Zugriffsanfrage stellt die Automatisierungseinrichtung einen temporären Zugang her, indem ein Token generiert wird, der dem zugreifenden Endgerät mitgeteilt wird, worauf das Endgerät mit Hilfe des Tokens eine Verbindung zur Automatisierungseinrichtung aufbaut, deren Zugriffsschutz den Token erkennt und den Zugang ermöglicht, worauf der generierte Token für weitere Zugriffe ungültig gemacht wird.



DE 102 00 681 A 1

3NSDOCID: <DE_____10200681A1_I_>

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät auf eine Automatisierungseinrichtung, die über eine physikalische Netzwerkverbindung miteinander verbunden sind, sowie eine dazu korrespondierende Automatisierungseinrichtung.

[0002] Im Service- oder Fehlerfall wird häufig seitens einer Service-Hotline (Teleservice) eine Online-Verbindung auf Daten oder Programme einer Automatisierungseinrichtung (AE) benötigt. Eine Automatisierungseinrichtung kann z. B. eine Werkzeugmaschine, eine Produktionsmaschine oder eine speicherprogrammierbare Steuerung sein. Ein Endgerät kann dabei prinzipiell jedes Gerät (im allgemeinen einen PC) sein, auf dem eine nicht näher spezifizierte Applikation läuft, die ein Service-Techniker zur Erfüllung seiner Aufgabe einsetzt und die eine Online-Verbindung auf die Automatisierungseinrichtung benötigt.

[0003] Diese Online-Verbindung wird heute über Modem und Telefonleitung hergestellt. Bekannte Programme wie "ReachOut" oder "NetMeeting" ermöglichen dann online die Fernsteuerung von Applikationen auf der Automatisierungseinrichtung oder den Transfer von Daten.

[0004] Die Darstellung gemäß der **Fig. 2** zeigt ein Blockschaltbild mit einer solchen bekannten Anordnung mit einer Automatisierungseinrichtung **1**, welche über ein erstes Modem **2** mit einem Telefonnetz **3** verbunden ist. Auf der anderen Seite ist ein Endgerät **5** gezeigt, das ebenfalls über ein Modem **4** mit dem Telefonnetz **3** in Verbindung steht.

[0005] In den meisten Fällen bestehen seitens des Betreibers der Automatisierungseinrichtung **1** hohe Sicherheitsanforderungen, die alleine durch Vergabe eines Logins und eines Passworts nur unzureichend befriedigt werden. Dieses Verfahren hat die folgenden Nachteile:

- wer in Besitz von Login und Passwort ist, kann sich auf der Automatisierungseinrichtung einloggen. Es gibt auf Seite der Automatisierungseinrichtung keine Kontrolle, wer sich einwählt, d. h. von wo aus angerufen wird,
- Login und Passwort sind in der Regel zeitlich unbegrenzt gültig,
- Daten werden unverschlüsselt übertragen.

[0006] Das Sicherheitsproblem wurde daher bisher einfach durch physikalische Trennung der Online-Verbindung gelöst, d. h. durch Ziehen des Modemsteckers, was in **Fig. 2** durch die gestrichelte Linie zwischen Telefonnetz **3** und dem Modem **2** angedeutet ist.

[0007] Durch die zunehmende Integration von Automatisierungseinrichtungen in eine Netz-Infrastruktur wie Intranet oder Internet werden keine Modemverbindungen mehr benötigt. Dadurch entsteht das zusätzliche Problem, dass die zum Betrieb der Automatisierungseinrichtung notwendige physikalische Netzverbindung nicht mehr jederzeit getrennt werden kann.

[0008] Die Anwendung des temporären Passwortverfahrens ist bei Internet Verbindung besonders vorteilhaft, kann aber auch bei Modemverbindungen (z. B. wenn der Stecker nicht gezogen werden kann) sinnvoll sein.

[0009] Ein weiterer Vorteil der Erfindung ist, dass keine Benutzeradministration notwendig ist. Für den Zugriff von außen ist es nicht notwendig, dass ein Administrator einen Benutzer für einen Servicetechniker einrichtet (und nicht vergisst, den Benutzer wieder zu löschen, wenn der Account nicht mehr benötigt wird).

[0010] Die Darstellung gemäß der **Fig. 3** zeigt ein Blockschaltbild einer solchen Anordnung. Eine Automatisierungseinrichtung **1** ist mit einem Intranet (z. B. über Ethernet) verbunden. Das Intranet besitzt einen Zugang zu einem Internet **7**, an das wiederum ein Endgerät **5** angeschlossen ist. Somit besteht eine physikalische Netzwerkverbindung zwischen der Automatisierungseinrichtung **1** und dem Endgerät **5**. Eine Absicherung ist nur durch eine anlagenweite Firewall **8** zwischen dem Intranet **6** und dem Internet **7** möglich, hingegen keine physikalische Trennung.

[0011] Eine Firewall steht als Bezeichnung für alle Schutzmaßnahmen (Hard- und Software), die ein Netzwerk (z. B. ein lokales Netzwerk LAN oder ein Intranet mit angeschlossenen Servern innerhalb eines Unternehmens) von einem anderen (z. B. dem weltweiten Internet außerhalb des Unternehmens oder Einwahlroutern über das ISDN zum Remote-Zugriff für Tele-Worker) abschotten. Ziele sind die Verhinderung unerlaubten Zugriffs auf sensible Daten, Verhinderung von Datenverlust und Verhindern des Einschleppens von Computerviren.

[0012] Daran wird deutlich, dass eine Firewall aufgrund der Vielzahl der Aufgaben nicht die gleiche Sicherheit bieten kann, wie eine physikalische Trennung der Verbindung. Eine solche ist jedoch, wie bereits erwähnt, in einer Konstellation gemäß **Fig. 3** nicht jederzeit möglich.

[0013] Eine Firewall bietet i. d. R. keine Zugriffsschutzmechanismen. In unserem Szenario wäre der Zugriff über eine Firewall auf das Automatisierungsgerät freigeschaltet, um Zugriff von außen zu ermöglichen.

[0014] Aufgabe der vorliegenden Erfindung ist es daher, einen ausreichend Zugriffsschutz für eine solche Automatisierungseinrichtung zu schaffen, der auch ohne eine physikalische Trennung der Verbindung eine vergleichbare Sicherheit bietet.

[0015] Diese Aufgabe wird gemäß der Erfindung durch ein Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät auf eine Automatisierungseinrichtung gelöst, die über eine physikalische Netzwerkverbindung miteinander verbunden sind, wobei die Automatisierungseinrichtung über einen Zugriffsschutz verfügt, der in einem Grundzustand jeden Zugang über die Netzwerkverbindung abweist, wobei die Automatisierungseinrichtung auf eine Zugriffsanfrage einen temporären Zugang herstellt, indem ein Token generiert wird, der dem zugreifenden Endgerät mitgeteilt wird, worauf das Endgerät mit Hilfe des Tokens eine Verbindung zur Automatisierungseinrichtung aufbaut, deren Zugriffsschutz den Token erkennt und den Zugang ermöglicht, worauf der generierte Token für weitere Zugriffe ungültig gemacht wird.

[0016] Die Tokengenerierung kann entweder durch das Automatisierungsgeräte selbst oder durch eine externe Einheit erfolgen (vgl. Verfahren zum RLA Access in Siemens LANs, bei dem durch eine Scheckkarte Nummern erzeugt wird). Das Automatisierungsgerät überprüft die Gültigkeit des Tokens entweder durch den Vergleich mit einem lokal abgelegtem Token oder durch andere Kriterien wie zeitliche Synchronität oder Prüfsummen.

[0017] Dabei erfordert vorzugsweise eine Zugriffsanfrage eines Endgerätes eine Identifizierung gegenüber der Automatisierungseinrichtung, die geprüft wird, bevor diese einen Token generiert.

[0018] Weiter hat es sich als besonders sicher erwiesen, wenn eine Mitteilung eines generierten Tokens in verschlüsselter Form über die physikalische Netzwerkverbindung erfolgt.

[0019] Die Sicherheit lässt sich noch weiter steigern, wenn eine Mitteilung eines generierten Tokens über eine von der die Automatisierungseinrichtung und das Endgerät verbindenden physikalische Netzwerkverbindung unabhän-

gige andere Verbindung erfolgt.

[0020] Weiter hat es sich als günstig erwiesen, wenn das Endgerät mit Hilfe des Tokens eine verschlüsselte Verbindung zur Automatisierungseinrichtung aufbaut, insbesondere eine Verbindung mit Kanalverschlüsselung.

[0021] Der von der Automatisierungseinrichtung generierte Token kann entweder ein Passwort oder eine Geheimzahl/PIN oder eine Login/Passwort Kombination oder ein Sicherheitszertifikat sein. Daneben sind noch eine Vielzahl anderer tokenbasierter elektronischer Signaturmittel wie z. B. Smart-Cards etc. einsetzbar.

[0022] Die Sicherheit des erfindungsgemäßen Verfahrens lässt sich noch weiter steigern, indem jeder von der Automatisierungseinrichtung generierte Token von vornherein zeitlich nur begrenzt gültig ist.

[0023] Dies lässt sich weiter verbessern, indem eine Verbindung zwischen der Automatisierungseinrichtung und einem Endgerät ebenfalls zeitlich begrenzt ist.

[0024] Wie eingangs dargestellt, kann die physikalische Netzwerkverbindung zwischen der Automatisierungseinrichtung und einem Endgerät eine lokale Netzwerkverbindung, insbesondere ein Intranet sein oder eine Internet-Netzwerkverbindung.

[0025] Ferner wird die Aufgabe der Erfindung durch eine Automatisierungseinrichtung zum Anschluss an eine physikalische Netzwerkverbindung mit einem Zugriffsschutz gelöst, durch den

- ein Zugriff auf die Automatisierungseinrichtung sperrbar ist,
- die Identität eines anfragenden Endgerätes verifizierbar ist,
- auf Anforderung ein für einen einmaligen Zugriff gültiger Token generierbar ist,
- im Falle eines Zugriffsversuchs die Gültigkeit eines solchen Tokens verifizierbar ist und dieser Token nach einmaligem erfolgreichen Aufbau einer Verbindung ungültig machbar ist.

[0026] Die Erfindung lässt sich besonders gut zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät auf eine Automatisierungseinrichtung zur Durchführung eines Teleservice von einem Endgerät auf der Automatisierungseinrichtung verwenden.

[0027] Weitere Vorteile und Details der Erfindung ergeben sich anhand der folgenden Ausführungen und in Verbindung mit der weiteren Figur. Es zeigt jeweils in Prinzipdarstellung:

[0028] **Fig.** 1 ein Blockschaltbild einer erfindungsgemäßen Automatisierungseinrichtung mit Zugriffsschutz,

[0029] **Fig.** 2 ein Blockschaltbild einer herkömmlichen Anbindung einer Automatisierungseinrichtung an ein Telefonnetz über Modems und

[0030] **Fig.** 3 ein Blockschaltbild einer aktuellen Anbindung einer Automatisierungseinrichtung an eine Netz-Infrastruktur mit Intranet und Internet mit Absicherung durch eine Firewall.

[0031] Die Darstellungen von **Fig.** 2 und **Fig.** 3 wurden bereits eingangs beschrieben. Die **Fig.** 3 zeigt nun eine erfindungsgemäße Anordnung mit einer Automatisierungseinrichtung **1**, mit der über ein Intranet **6** und ein Internet **7** ein Endgerät **5** physikalisch verbunden ist. Die erfindungsgemäßen Maßnahmen sind nun innerhalb der Automatisierungseinrichtung **1** realisiert.

[0032] Auf der Automatisierungseinrichtung wird ein Zugriffsschutz **10** installiert, z. B. in Form einer Zusatz-Software, die im Grundzustand keine Verbindung von außen auf die Automatisierungseinrichtung **1** zulässt. Durch einen einfachen Bedienvorgang (keine Administrator-Rechte notwendig, keine Benutzerverwaltung notwendig) kann über einen Tokengenerator **9**, der ebenfalls im Rahmen des Zugriffsschutzes **10** realisiert sein kann, ein Token erzeugt werden, mit dem der Zugriff von außen freigegeben werden kann. Ein Token kann dabei z. B. ein Passwort, eine Login/Passwort Kombination oder auch ein Sicherheits-Zertifikat etc. sein.

[0033] Dabei erfüllt das Token vorzugsweise zumindest teilweise die folgenden Sicherheitsanforderungen:

- die Gültigkeit des Tokens ist zeitlich begrenzt,
  die Gültigkeit des Tokens ist auf einmalige Verwendung eingeschränkt,
- die Gesamtdauer der Online-Verbindung kann zeitlich begrenzt werden (das Endgerät **5** erhält eine Warnung kurz vor Trennung der Verbindung),
- der Zugang wird nur für einen bestimmten Client freigegeben (Identifikation z. B. anhand der IP-Adresse),
- das Token wird für jede Online-Verbindung neu erzeugt, so dass dieses für spätere Sessions nicht mehr verwendet werden kann,
- die Generierung des Tokens kann nur an der AE selbst erfolgen,
- die Daten werden verschlüsselt (Secure Socket Layer SSL mit 128 Bit Schlüssel).

[0034] Die Abkürzung SSL steht dabei für "Secure Sokkets Layer" und bezeichnet ein Verfahren zur Sicherung von Datenübertragung im Rahmen des Internet. Dabei wird der Datenstrom nach einem Handshake zu Beginn einer Verbindung unmittelbar auf der Bitebene durch Verschlüsselung gesichert. Das Verschlüsselungsverfahren für die zu übertragenden Daten selbst basiert auf bekannten Verfahren. Am Ende einer Verbindung erfolgt ein zweiter Handshake. Der unbefugte Zugriff auf dem Übertragungsmedium wird durch SSL verhindert, weshalb man auch von einer Kanalverschlüsselung spricht.

[0035] Das Ziehen des Modemsteckers wird somit durch eine Zugangssoftware ersetzt, die im Grundzustand jeden Zugang abweist.

[0036] Damit lässt sich dann folgendes Szenario realisieren. Ein Wartungstechniker vor Ort benötigt bei der Beseitigung einer Störung die Hilfe der Service-Hotline. Der Service-Techniker benötigt wiederum einen Online-Zugang auf die Automatisierungseinrichtung, um die Störung genauer zu analysieren. Grundsätzlich besteht eine physikalische Netzverbindung (Internet) zwischen Automatisierungseinrichtung und Service-Hotline, allerdings besteht kein Zugang (Login u. Passwort).

[0037] Der Servicetechniker bittet den Wartungstechniker nun (z. B. per Telefon oder E-Mail), einen temporären Zugang herzustellen, und gibt dazu seine IP-Adresse zur Identifizierung an. Dieser erzeugt daraufhin vor Ort das temporäre Login mit Passwort. Login und Passwort werden dem Servicetechniker mitgeteilt. Sobald sich der Servicetechniker einloggt, wird eine verschlüsselte Verbindung aufgebaut und damit das Login ungültig.

Patentansprüche

1. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1), die über eine physikalische Netzwerkverbindung (3; 6, 7) miteinander verbunden sind, wobei die Automatisierungseinrichtung über einen Zugriffsschutz (10) verfügt, der in einem Grundzustand

jeden Zugang über die Netzwerkverbindung (3; 6, 7) abweist, wobei die Automatisierungseinrichtung auf eine Zugriffsanfrage einen temporären Zugang herstellt, indem ein Token (9) generiert wird, der dem zugreifenden Endgerät mitgeteilt wird, worauf das Endgerät mit Hilfe des Tokens eine Verbindung zur Automatisierungseinrichtung aufbaut, deren Zugriffsschutz (10) den Token erkennt und den Zugang ermöglicht, worauf der generierte Token für weitere Zugriffe ungültig gemacht wird.

2. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach Anspruch 1, wobei eine Zugriffsanfrage eines Endgerätes eine Identifizierung gegenüber der Automatisierungseinrichtung (1) erfordert, die geprüft wird, bevor diese (1) einen Token generiert.

3. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach Anspruch 1 oder 2, wobei eine Mitteilung eines generierten Tokens in verschlüsselter Form über die physikalische Netzwerkverbindung (3; 6, 7) erfolgt.

4. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach Anspruch 1 oder 2, wobei eine Mitteilung eines generierten Tokens über eine von der die Automatisierungseinrichtung (1) und das Endgerät (5) verbindenden physikalische Netzwerkverbindung (3; 6, 7) unabhängige andere Verbindung erfolgt.

5. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der vorangehenden Ansprüche, wobei das Endgerät mit Hilfe des Tokens eine verschlüsselte Verbindung zur Automatisierungseinrichtung aufbaut, insbesondere eine Verbindung mit Kanalverschlüsselung.

6. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der vorangehenden Ansprüche, wobei der von der Automatisierungseinrichtung (1) generierte Token (9) ein Passwort oder eine Geheimzahl/PIN ist.

7. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der vorangehenden Ansprüche 1 bis 5, wobei der von der Automatisierungseinrichtung (1) generierte Token (9) eine Login/Passwort Kombination ist.

8. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der vorangehenden Ansprüche 1 bis 5, wobei der von der Automatisierungseinrichtung (1) generierte Token (9) ein Sicherheitszertifikat ist.

9. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der vorangehenden Ansprüche, wobei jeder von der Automatisierungseinrichtung (1) generierte Token (9) zeitlich begrenzt gültig ist.

10. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der vorangehenden Ansprüche, wobei eine Verbindung zwischen der Automatisierungseinrichtung (1) und einem Endgerät (5) zeitlich begrenzt ist.

11. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der vorangehenden Ansprüche, wobei die physikalische Netzwerkverbindung zwischen der Automatisierungseinrichtung (1) und einem Endgerät (5) eine lokale Netzwerkverbindung, insbesondere ein Intranet (6), ist.

12. Verfahren zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der vorangehenden Ansprüche, wobei die physikalische Netzwerkverbindung zwischen der Automatisierungseinrichtung (1) und einem Endgerät (5) eine Internet-Netzwerkverbindung (7) ist.

13. Automatisierungseinrichtung (1) zum Anschluss an eine physikalische Netzwerkverbindung (3; 6, 7) mit einem Zugriffsschutz (10), durch den
ein Zugriff auf die Automatisierungseinrichtung (1) sperrbar ist,
die Identität eines anfragenden Endgerätes (5) verifizierbar ist,
auf Anforderung ein für einen einmaligen Zugriff gültiger Token generierbar ist,
im Falle eines Zugriffsversuchs die Gültigkeit eines solchen Tokens verifizierbar ist und dieser Token nach einmaligem erfolgreichen Aufbau einer Verbindung ungültig machbar ist.

14. Verwendung eines Verfahrens zum sicheren Aufbau eines temporären Zugriffs von einem Endgerät (5) auf eine Automatisierungseinrichtung (1) nach einem der Ansprüche 1 bis 12 zur Durchführung eines Teleservice von einem Endgerät auf der Automatisierungseinrichtung.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 102 00 681 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 31. Juli 2003

FIG 1

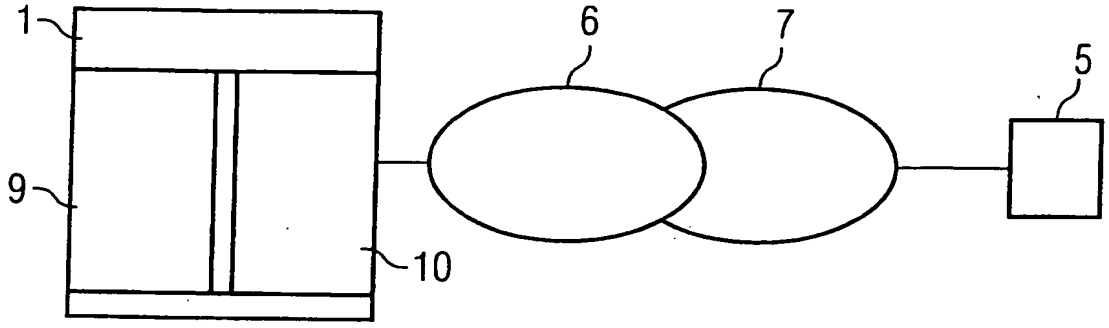


FIG 2

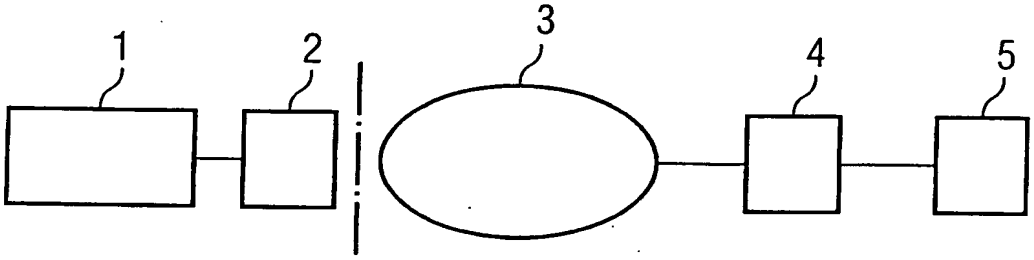


FIG 3